J1

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/801,962	03/15/2004	Brant Candelore	80398P577	2553

8791 7590 01/29/2007
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER
BAUM, RONALD

ART UNIT	PAPER NUMBER
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/29/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/801,962	**Applicant(s)** CANDELORE, BRANT	
	Examiner Ronald Baum	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7,9-12,14,15,17-31,36-47,49 and 50* is/are rejected.

7)☒ Claim(s) *6,8,13,16,32-35,48* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-50 are pending for examination.

2. Claims 1-5,7,9-12,14,15,17-31,36-47,49 and 50 are rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-5,7,9-12,14,15 are rejected under 35 U.S.C. 102(b) as being anticipated by Enichen et al, U.S. Patent 6,333,983 B1.

4. As per claim 1; "A method comprising:

receiving a decoded scrambling key

having a key size according to

a first cryptographic protocol [figures 5-19 and accompanying descriptions, whereas the use of weak/strong derived keys and associated transport, KEK, etc., in the at least DES cryptographic environment (i.e., cryptographic protocol) insofar as the said keys are size adjusted (i.e., single/double length) dependent on the cryptographic primitives used, clearly encompasses the claim limitations, as broadly interpreted by the examiner.];

reducing the key size of the decoded scrambling key

to match a key size of a second cryptographic protocol to form a reduced key size descrambling key

whose value is a function of

every bit of the decoded scrambling key[figures 5-19 and accompanying descriptions, whereas the use of weak/strong derived keys and associated transport, KEK, etc., in the at least DES cryptographic environment (i.e., first/second cryptographic protocols; single or multiple encrypted/decrypted) insofar as the said keys are size adjusted (i.e., single/double length) dependent on the cryptographic primitives used, clearly encompasses the claim limitations, as broadly interpreted by the examiner.]; and

descrambling received scrambled content according to

the reduced key size descrambling key [figures 5-19 and accompanying descriptions, whereas the use of the DES cryptographic environment insofar as key management functions are performed for the sake of application to associated encryption/decryption of associated content, clearly encompasses the claim limitations, as broadly interpreted by the examiner.].".

As per claim 9, this claim is the embodied software of claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection; "An article of manufacture including a machine readable medium having stored thereon instructions which may be used to program a system to perform a method, comprising:

receiving a decoded scrambling key

having a key size according to

a first cryptographic protocol

to form a reduced key size descrambling key;

reducing the key size of the decoded scrambling key

to match a key size of a second cryptographic protocol

whose value is a function of

every bit of the decoded scrambling key; and

descrambling received scrambled content according to

the reduced key size descrambling key.".

5. Claim 2 ***additionally recites*** the limitation that; "The method of claim 1, wherein reducing the key size comprises:

dividing the decoded scrambling key into

a lower M-bits and

an upper N-bits;

performing a logical exclusive OR operation of

the upper N-bits across

the lower M-bits

to form an M-bit descrambling key as

the reduced key size descrambling key.".

The teachings of Enichen et al suggest such limitations (figures 5-19 and accompanying descriptions, whereas the use of weak/strong derived keys and associated transport, KEK, etc., in the at least DES cryptographic environment (i.e., cryptographic protocol) insofar as the said keys are size adjusted (i.e., '... dividing the decoded scrambling key' lower/upper M/N bits, of which DES inherently performs logical XOR operations at the sub-key generation/schedule level), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

As per claim 10, this claim is the embodied software of claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection; "The article of manufacture of claim 9, wherein reducing the key size comprises:

dividing the decoded scrambling key into

a lower M-bits and

an upper N-bits;

performing a logical exclusive OR operation of

the upper N-bits across

the lower M-bits

to form an M-bit descrambling key as

the reduced key size descrambling key.".

As per claim 4, this claim is the multiple iteration variation of claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection insofar as multiple encryption variations of DES would encompass the iterative aspects of the claim; "The method of claim 1, wherein reducing the key size comprises:

dividing the decoded descrambling key into a lower M-bits and

an upper M-bits;

performing a logical exclusive OR operation on

the lower M-bits and

the upper M-bits

to form an M-bit descrambling key;

dividing the M-bit descrambling key into

a lower X-bits and

an upper Y-bits; and

performing a logical exclusive OR operation of

the upper Y-bits across

the lower X-bits

to form an X-bit descrambling key as

the reduced key size descrambling key.".

As per claim 12, this claim is the embodied software of claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection; "The article of manufacture of claim 9, wherein reducing the key size comprises:

dividing the decoded descrambling key into

a lower M-bits and

an upper N-bits;

performing a logical exclusive OR operation on the lower M-bits and

the upper N-bits

to form an M-bit descrambling key;

dividing the M-bit descrambling key into

a lower X-bits and

an upper Y-bits; and

performing a logical exclusive OR operation of

the upper Y-bits across

the lower X-bits

to form an X-bit descrambling key as

the reduced key size descrambling key.".

6. Claim 3 ***additionally recites*** the limitation that; "The method of claim 1, wherein reducing the key size comprises:

dividing the decoded descrambling key into

a lower M-bits and

an upper M-bits;

performing a logical XOR operation on

the lower M-bits and

the upper M-bits

to form an M-bit descrambling key as

the reduced key size descrambling key.".

The teachings of Enichen et al suggest such limitations (figures 5-19 and accompanying descriptions, whereas the use of weak/strong derived keys and associated transport, KEK, etc., in the at least DES cryptographic environment (i.e., cryptographic protocol) insofar as the said keys are size adjusted (i.e., '… dividing the decoded scrambling key' lower/upper M bits, of which DES inherently performs logical XOR operations at the sub-key generation/schedule level), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

As per claim 11, this claim is the embodied software of claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection; "The article of manufacture of claim 9, wherein reducing the key size comprises:

dividing the decoded descrambling key into

a lower M-bits and

an upper M-bits;

performing a logical exclusive OR operation on

the lower M-bits and

the upper M-bits

to form an M-bit descrambling key as

the reduced key size descrambling key.".

7. Claim 5 ***additionally recites*** the limitation that; "The method of claim 1, wherein reducing the key size comprises:

hashing the bits of the decoded scrambling key; and selecting bits from the hash

to form the reduced key size descrambling key.".

The teachings of Enichen et al suggest such limitations (figures 5-19 and accompanying descriptions, whereas the use of weak/strong derived keys and associated transport, KEK, etc., in the at least DES cryptographic environment (i.e., cryptographic protocol) insofar as the said keys are size adjusted (i.e., DES inherently performs table selection/substitution/hash operations at the sub-key generation/schedule level), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

As per claim 14, this claim is the embodied software of claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection; "The article of manufacture of claim 9, wherein reducing the key size comprises:

hashing the bits of the decoded scrambling key; and

selecting bits from the hash

to form the reduced key size descrambling key.".

8. Claim 7 ***additionally recites*** the limitation that; "The method of claim 1, wherein

the first cryptographic protocol is a triple data encryption standard protocol (3DES) and

the second cryptographic protocol is one of

a digital video broadcast (DVB) common scrambling algorithm (CSA) and

a data encryption standard (DES) algorithm.".

The teachings of Enichen et al suggest such limitations (figures 5-19 and accompanying descriptions; whereas the use of the at least DES cryptographic environment (i.e., first/second cryptographic protocols; single or multiple encrypted/decrypted), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

As per claim 15, this claim is the embodied software of claim 7 above, and is rejected for the same reasons provided for the claim 7 rejection; "The article of manufacture of claim 9, wherein

the first cryptographic protocol is a triple data encryption standard protocol (3DES) and

the second cryptographic protocol is one of

a digital video broadcast (DVB) common scrambling algorithm (CSA) and

a data encryption standard (DES) algorithm.".

9. Claims 17-31,36-40 are rejected under 35 U.S.C. 102(b) as being anticipated by Ober et al, U.S. Patent 6,307,936 B1.

10. As per claim 17; "An integrated circuit comprising:

a first cryptographic block that may be iterated without limit

to descramble received information

using one of

an internal key and

a preprogrammed key

to form one of

a descrambled key and

descrambled data [figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for 'highly layered and complex … key management (i.e., col. 1,lines 58-col. 2,line 14)' and associated storage/access configurability internally or externally, clearly encompasses the claim limitations, as broadly interpreted by the examiner.];

a key feedback path

to store the descrambled key as

an internal key and

to provide

the one of

the internal key and

the preprogrammed key

to a key input of

the first cryptographic block [figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for 'highly layered and complex … key management (i.e., col. 1,lines 58-col. 2,line 14)' and associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, clearly encompasses the claim limitations, as broadly interpreted by the examiner.]; and

a second cryptographic block

to descramble received scrambled digital content

using a final descrambling key from

the first cryptographic block

to form

descrambled digital content [figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation is subsequently used for, and in support of, the content encryption/decryption, clearly encompasses the claim limitations, as broadly interpreted by the examiner.].".

11. Claim 18 ***additionally recites*** the limitation that; "The integrated circuit of claim 17, further comprising:

a data feedback path

to store the descrambled data within

a data register as internal data;

data selection logic

coupled to

the data register and

an external information input,

the data selection logic

to provide one of

internal data from

the data register and

received information from

the external information

input to

a data input of

the first cryptographic block.".

The teachings of Ober et al suggest such limitations (figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, and associated intermediate storage as utilized in the key processing, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

12. Claim 19 ***additionally recites*** the limitation that; "The integrated circuit of claim 17, wherein the key feedback path further comprises:

a preprogrammed key register

to store at least the preprogrammed key;

an internal key register

to store at least the descrambled key; and key selection logic

to provide the one of

the preprogrammed key and

the internal key

to the key input of

the first cryptographic block

using controls

accessible outside the integrated circuit and

accessible by an insecure CPU.".

The teachings of Ober et al suggest such limitations (figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, and associated intermediate internal data routing, selection and storage as utilized in the key processing, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

13. Claim 20 ***additionally recites*** the limitation that; "The integrated circuit of claim 17, further comprising:

gate enable logic

coupled to

the key feedback path of

the first cryptographic block

to receive the one of

the internal key and

the preprogrammed key; and

a logic gate

coupled to

a data output of

the first cryptographic block,

the logic gate

to compute a key hash value from the one of

the internal key and

the preprogrammed key

received from

the gate enable logic and the descrambled key received from the data output of the first cryptographic block when enabled by the gate enable logic.".

The teachings of Ober et al suggest such limitations (figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, and associated intermediate internal data routing, selection and storage as utilized in the key processing, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

14. Claim 21 ***additionally recites*** the limitation that; "The integrated circuit of claim 17, further comprising:

gate enable logic

coupled to

the data input of

the first cryptographic block

to receive the received information; and

a logic gate

coupled to

a data output of the first cryptographic block,

the logic gate

to compute a hash data value from

the received information and

the descrambled data from the data output of the first cryptographic block when enabled by the gate enable logic.".

The teachings of Ober et al suggest such limitations (figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, and associated intermediate internal data routing, selection and storage as utilized in the key processing, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

15. Claim 22 ***additionally recites*** the limitation that; "The integrated circuit of claim 17, further comprising:

a data feedback path to store at least

the descrambled data within

a data register;

gate enable logic coupled to

the data register; and

a logic gate coupled to

a data input of the first cryptographic block,

the logic gate

to form a permuted value from

the received information and

the descrambled data from the gate enable logic and

to provide the permuted value to

the data input of

the first cryptographic block when

enabled by the gate enable logic and

to provide the received information to

the data input of

the first cryptographic block when

disabled.".

The teachings of Ober et al suggest such limitations (figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, and associated intermediate internal data routing, selection and storage as utilized in the key processing, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

16. Claim 23 ***additionally recites*** the limitation that; "The integrated circuit of claim 17, further comprising:

gate enable logic to receive an internal data value;

a logic gate coupled to

the key feedback path of the first cryptographic block and

the gate enable logic,

the logic gate

to compute a permuted key value from

the internal data value and

the one of

the internal key and

the preprogrammed key when enabled by the gate enable logic and

to provide the permuted key value to

the key input of

the first cryptographic block; and

an external data register coupled to

a data output of the first cryptographic block

to store descrambled data generated by

the first cryptographic block with

the permuted key value received as

the key input of the first cryptographic block.".

The teachings of Ober et al suggest such limitations (figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, and associated intermediate internal data routing, selection and storage as utilized in the key processing, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

17. Claim 24 ***additionally recites*** the limitation that; "The integrated circuit of claim 17, wherein the first cryptographic block is

an embedded cryptographic CPU programmed to

iteratively descramble the received information

using one of

the internal key and

the preprogrammed key

to form one of

the descrambled key and

descrambled data; and

wherein

the key feedback path and

a data feedback path

to operate according to

an off-chip insecure CPU.".

The teachings of Ober et al suggest such limitations (figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, and associated intermediate internal data routing (either initiated internally or as a result of external IC interaction), selection and storage as utilized in the key processing, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

18. Claim 25 ***additionally recites*** the limitation that; "The integrated circuit of claim 18, wherein

the key feedback path and

the data feedback path

to operate according to

an off-chip insecure CPU.".

The teachings of Ober et al suggest such limitations (figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, and associated intermediate internal data routing (either initiated internally or as a result of external IC interaction), selection and storage as utilized in the key processing, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

19. Claim 26 ***additionally recites*** the limitation that; "The integrated circuit of claim 17,
wherein the first cryptographic block is
to operate according to
a state machine; and
wherein
the key feedback path and
a data feedback path
to operate according to
an off-chip insecure CPU.".

The teachings of Ober et al suggest such limitations (figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor (i.e., inherently a "a state machine") insofar as the key management/creation allows for associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, and associated intermediate internal data routing (either initiated internally or as a result of external IC interaction), selection and storage as utilized in the key processing, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

20. Claim 27 ***additionally recites*** the limitation that; "The integrated circuit of claim 23, wherein

the internal value being one of

a fixed value,

a stored internal key,

stored internal data, and

a one-time-programmable value.".

The teachings of Ober et al suggest such limitations (figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, and associated intermediate internal data routing (either initiated internally or as a result of external IC interaction), selection and storage as utilized in the key processing, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

21. Claim 28 ***additionally recites*** the limitation that; "The integrated circuit of claim 17, further comprising:

gate enable logic to receive an internal data value;

a logic gate

coupled to the key feedback path of the first cryptographic block and the gate enable logic,

the logic gate

to compute a permuted key value from

the internal data value and

the one of

the internal key and

the preprogrammed key

when enabled by

the gate enable logic and

to provide the permuted key value to the key input of the first cryptographic block to generate the final key and to provide the final key as a key input of the second cryptographic block.".

The teachings of Ober et al suggest such limitations (figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, and associated intermediate internal data routing (either initiated internally or as a result of external IC interaction), selection and storage as utilized in the key processing, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

22. Claim 29 ***additionally recites*** the limitation that; "The integrated circuit of claim 28, wherein

the internal value being one of

a fixed value,

a stored internal key,

stored internal data, and

a one-time-programmable value.".

The teachings of Ober et al suggest such limitations (figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, and associated intermediate internal data routing (either initiated internally or as a result of external IC interaction), selection and storage as utilized in the key processing, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

23. Claim 30 ***additionally recites*** the limitation that; "The integrated circuit of claim 17, further comprising:

a logic gate

to receive

the descrambling key from

the first cryptographic block and

an internal value,

the logic gate

to generate a permuted key value as

the final key and

provide the final key to

a key input of

the second cryptographic block.".

The teachings of Ober et al suggest such limitations (figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, and associated intermediate internal data routing (either initiated internally or as a result of external IC interaction), selection and storage as utilized in the key processing, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

24. Claim 31 ***additionally recites*** the limitation that; "The integrated circuit of claim 30, wherein

the internal value being one of

a fixed value,

a stored internal key,

stored internal data, and

a one-time-programmable value.".

The teachings of Ober et al suggest such limitations (figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, and associated intermediate internal data routing (either initiated internally or as a result of external IC interaction), selection and storage as utilized in the key processing, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

25. Claim 36 ***additionally recites*** the limitation that; "The integrated circuit of claim 17, wherein

the integrated circuit is

a decoder integrated circuit

to decompress

the descrambled digital content.".

The teachings of Ober et al suggest such limitations (figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, and associated intermediate internal data routing (either initiated internally or as a result of external IC interaction), selection and storage as utilized in the key processing, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

26. Claim 37 ***additionally recites*** the limitation that; "The integrated circuit of claim 17, wherein

the integrated circuit is

a cryptographic integrated circuit.".

The teachings of Ober et al suggest such limitations (figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, and associated intermediate internal data routing (either initiated internally or as a result of external IC interaction), selection and storage as utilized in the key processing, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

27. Claim 38 ***additionally recites*** the limitation that; "The integrated circuit of claim 17, further comprising:

a decoder to decode

the descrambled digital content to form

clear digital content.".

The teachings of Ober et al suggest such limitations (figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, and associated intermediate internal data routing (either initiated internally or as a result of external IC interaction), selection and storage as utilized in the key processing, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

28. Claim 39 ***additionally recites*** the limitation that; "The integrated circuit of claim 38, further comprising:

a non-volatile memory to store

the clear digital content in

a scrambled format.".

The teachings of Ober et al suggest such limitations (figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, and associated intermediate internal data routing (either initiated internally or as a result of external IC interaction), selection and storage as utilized in the key processing, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

29. Claim 40 ***additionally recites*** the limitation that; "The integrated circuit of claim 17, wherein

the preprogrammed key is

a one-time programmable value

that cannot be read or overwritten once programmed.".

The teachings of Ober et al suggest such limitations (figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for associated storage/access configurability internally or externally, inclusive of key manipulation sub-processes, and associated intermediate internal data routing (either initiated internally or as a result of external IC interaction), selection and storage as utilized in the key processing, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 41-47,49 and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, U.S. Patent 5,825,879, and further in view of Ober et al, U.S. Patent 6,307,936 B1.

Davis discloses a secure/encryption oriented video content processor/set-top box (i.e., secure content rendering in the broad sense) for secure content transport to the set-top box, inclusive of the unit receiver, digital processing elements, cryptographic processing encryption/decryption elements (and associated key management aspects), etc. However, Davis fails to disclose the encryption/decryption/key management/creation aspects of the set-top box as recited in the claims per se.

Ober et al teaches of the management/creation of keys in a cryptographic co-processor as detailed in the above claim rejections.

The examiner asserts that it would have been obvious to one ordinary skill in the art at the time the invention was made to encompass the Ober et al management/creation of keys in a cryptographic co-processor teachings as applied to the Davis set-top box in order to assure a more robust and cryptographically secure set-top box.

Such motivation exists because the Davis set-top box security, of which a requirement for as secure a form of cryptographic protection of content is required, is obviously enhanced via the Ober et al management/creation of keys cryptographic co-processor as an integral part of the set-top box.

30. As per claim 41; "A set-top box, comprising:

a tuner

to receive scrambled content;

a CPU; and

an integrated circuit

select at least one of

a preprogrammed key,

internal key,

external data and

internal data

under control of the CPU, comprising:

a first cryptographic block

to descramble received information

using one of

an internal key and

a preprogrammed key

to form one of

a descrambled key and

descrambled data,

a key feedback path

to iteratively store the descrambled information

as one of

an internal key and

internal data, and

to provide

the one of

the internal key and

the preprogrammed key

to a key input of

the first cryptographic block and

to provide

the one of

external data and

the internal data

to a data input of

the first cryptographic block,

a second cryptographic block

to descramble received scrambled digital content

using a final descrambling key from

the first cryptographic block

to form

descrambled digital content, and

a decoder

to decode the descrambled digital content

to form

clear digital content.".

31. Claim 42 ***additionally recites*** the limitation that; "The set-top box of claim 41, further comprising:

a data feedback path

to store the descrambled data within

a data register as internal data;

data selection logic

coupled to

the data register and

an external information input,

the data selection logic

to provide one of

internal data from the data register and

received information from the external information input

to a data input of

the first cryptographic block.".

32. Claim 43 ***additionally recites*** the limitation that; "The set-top box of claim 41, wherein the key feedback path further comprises:

a preprogrammed key register

to store at least the preprogrammed key;

an internal key register

to store at least the descrambled key; and

key selection logic

to provide the one of

the preprogrammed key and

the internal key

to the key input of

the first cryptographic block.".

33. Claim 44 ***additionally recites*** the limitation that; "The set-top box of claim 41, further comprising:

gate enable logic coupled to

the key feedback path of

the first cryptographic block

to receive the one of

the internal key and

the preprogrammed key; and

a logic gate coupled to

a data output of

the first cryptographic block,

the logic gate

to compute a key hash value from

the one of

the internal key and

the preprogrammed key

received from

the gate enable logic and

the descrambled key received from

the data output of

the first cryptographic block when enabled by

the gate enable logic.".

34. Claim 45 ***additionally recites*** the limitation that; "The set-top box of claim 41, further comprising:

gate enable logic coupled to the data input of the first cryptographic block to receive the received information; and

a logic gate coupled to a data output of the first cryptographic block, the logic gate to compute a hash data value from the received information and the descrambled data from the data output of the first cryptographic block when enabled by the gate enable logic.".

35. Claim 46 ***additionally recites*** the limitation that; "The set-top box of claim 41, further comprising:

a data feedback path
to store at least
the descrambled data within
a data register;
gate enable logic
coupled to
the data register; and
a logic gate
coupled to
a data input of
the first cryptographic block,

the logic gate

to form a permuted value from the received information and the descrambled data from the gate enable logic and to provide the permuted value to the data input of the first cryptographic block when enabled by the gate enable logic and

to provide the received information to the data input of the first cryptographic block when disabled.".

36. Claim 47 ***additionally recites*** the limitation that; "The set-top box of claim 41, further comprising:

gate enable logic

to receive an external data value;

a logic gate

coupled to

the key feedback path of

the first cryptographic block and

the gate enable logic,

the logic gate

to compute a permuted key value from

the external data value and

the one of

the internal key and

the preprogrammed key

when enabled by

the gate enable logic and

to provide the permuted key value to

the key input of

the first cryptographic block; and

an external data register

coupled to

a data output of

the first cryptographic block

to store descrambled data generated by

the first cryptographic block with

the permuted key value received as

the key input of

the first cryptographic block.".

37. Claim 49 ***additionally recites*** the limitation that; "The set-top box of claim 41, further comprising:

a non-volatile memory to store

the clear digital content in

a scrambled format.".

38. Claim 50 ***additionally recites*** the limitation that; "The set-top box of claim 41, wherein

the preprogrammed key is

a one-time programmable value

that cannot be read or overwritten

once programmed.".

Allowable Subject Matter

39. Claims 6,8,13,16,32-35 and 48 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim 6 ***additionally recites*** the limitation that; "The method of claim 1, wherein

the first cryptographic protocol is

an advanced encryption standard protocol and

the second cryptographic protocol is one of

a triple data encryption standard protocol (3DES),

a digital video broadcast (DVB) common scrambling algorithm (CSA) and

a data encryption standard (DES) algorithm.".

As per claim 13, this claim is the embodied software of claim 6 above, and is objected to for the same reasons provided for the claim 6 objection; "The article of manufacture of claim 9, wherein the first cryptographic protocol is

an advanced encryption standard protocol and

the second cryptographic protocol is one of

a triple data encryption standard protocol (3DES),

a digital video broadcast (DVB) common scrambling algorithm (CSA) and

a data encryption standard (DES) algorithm.".

Claim 8 ***additionally recites*** the limitation that; "The method of claim 1, wherein

the first cryptographic protocol is

digital video broadcast (DVB) common scrambling algorithm (CSA) and

the second cryptographic protocol is

the data encryption standard (DES) algorithm.".

As per claim 16, this claim is the embodied software of claim 8 above, and is objected to for the same reasons provided for the claim 8 objection; "The article of manufacture of claim 9, wherein

the first cryptographic protocol is

digital video broadcast (DVB) common scrambling algorithm (CSA) and

the second cryptographic protocol is

the data encryption standard (DES) algorithm.".

Claim 32 ***additionally recites*** the limitation that; "The integrated circuit of claim 17, further comprising:

key reduction logic

to receive the descrambled key from the first cryptographic block having a key size according to a first cryptographic protocol of the first cryptographic block,

the key reduction logic

to reduce the key size of the descrambled key to match a key size of a second cryptographic protocol of the second cryptographic block to form the final key whose value is a function of every bit of the descrambled key.".

Claim 33 ***additionally recites*** the limitation that; "The integrated circuit of claim 32, wherein

the first cryptographic protocol is

an advanced encryption standard (AES) protocol and

the second cryptographic protocol is one of

a triple data encryption standard (3DES) protocol,

a digital video broadcast (DVB) common scrambling algorithm (CSA) protocol and

a data encryption standard (DES) protocol.".

Claim 34 ***additionally recites*** the limitation that; "The integrated circuit of claim 32, wherein the first cryptographic protocol is

a triple data encryption standard protocol (3DES) and

the second cryptographic protocol is one of

a digital video broadcast (DVB) common scrambling algorithm (CSA) and

a data encryption standard (DES) algorithm.".

Claim 35 ***additionally recites*** the limitation that; "The integrated circuit of claim 32, wherein

the first cryptographic protocol is

digital video broadcast (DVB) common scrambling algorithm (CSA) and

the second cryptographic protocol is

the data encryption standard (DES) algorithm.".

Claim 48 ***additionally recites*** the limitation that; "The set-top box of claim 41, wherein

the first cryptographic block and

the second cryptographic block

are logic operating in accordance with

an advanced encryption standard (AES).".

Conclusion

40. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov . The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov . Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

Ronald Baum

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/23/07